Michigan Law Review

Volume 107 | Issue 5

2009

Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act

Katherine Mesenbring Field
University of Michigan Law School

NOTE

AGENCY, CODE, OR CONTRACT: DETERMINING EMPLOYEES' AUTHORIZATION UNDER THE COMPUTER FRAUD AND ABUSE ACT

*Katherine Mesenbring Field**

The federal Computer Fraud and Abuse Act ("CFAA") provides for civil remedies against individuals who have accessed a protected computer without authorization or in excess of their authorization. With increasing numbers of employees using computers at work, employers have turned to the CFAA in situations where disloyal employees have pilfered company information from the employer's computer system. The vague language of the CFAA, however, has led courts to develop three different interpretations of "authorization" in these CFAA employment cases, with the result that factually similar cases in different courts can generate opposite outcomes in terms of employee liability under the statute. This Note examines the three alternative interpretations of authorization in CFAA employment cases and concludes that courts should generally employ a code-based interpretation as the default definition of authorization under the CFAA, with employment contracts that clearly outline the limits of employee computer access providing meaning to authorization in cases where courts in their discretion find it to be appropriate.

TABLE OF CONTENTS

* J.D. Candidate, May 2009. Special thanks to my family for their unending support as well as Professor J.J. Prescott, Leigh Wasserstrom, Lance Phillips, and Amie Medley for their helpful comments and advice throughout the process of writing this Note.

INTRODUCTION

Computers are widely used in the workplace for understandable reasons: they often increase productivity, making employees more efficient and effective at their jobs.[1] But by making information more accessible and shareable, computers and computer networks in the workplace increase the risk that certain information—confidential, proprietary, or trade secret information—may end up in the hands of competitors. In light of this risk, companies take preventative measures; they encode computer networks to discourage hackers and require employees to enable and utilize password protections to prevent use by outsiders. These preventative measures, however, do little to protect against one risk: that an employee himself will use his access to the company's computers and network to gather and turn over such confidential, proprietary, or trade secret information to competitors.

Yet while it may be difficult to fashion preventative measures to thwart the efforts of such a rogue employee, companies are increasingly finding that they can recoup the associated losses through the use of a federal computer-misuse statute. This statute, the Computer Fraud and Abuse Act ("CFAA"),[2] was originally developed to target computer hackers.[3] The CFAA also, however, allows private citizens to bring suits against a person who "intentionally accesses a computer *without authorization or exceeds authorized access*, and thereby obtains . . . information from any protected computer" or who "knowingly and with intent to defraud, *accesses a protected computer without authorization, or exceeds authorized access*."[4]

---

1. The most recent federal survey indicated that 77 million people in the United States use a computer at work. BUREAU OF LABOR STATISTICS, COMPUTER AND INTERNET USE AT WORK IN 2003, at 1 (2005), *available at* http://www.bls.gov/news.release/pdf/ciuaw.pdf. For a discussion of the link between IT use and productivity in the workplace, see Kevin J. Stiroh, *Information Technology and the U.S. Productivity Revival: What Do the Industry Data Say?*, 92 AM. ECON. REV. 1559 (2002).

2. 18 U.S.C. § 1030 (2006).

3. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 2 (2007) [hereinafter PROSECUTING COMPUTER CRIMES], *available at* http://www.usdoj.gov/criminal/cybercrime/ccmanual/.

4. 18 U.S.C. § 1030(a)(2)(C), (a)(4), (g) (emphasis added).

Thus, employers can bring their rogue employees into court, arguing under the rather general language in the CFAA that the employee was without authorization or exceeded his authorization to access the company computer system when he did so to obtain proprietary company information for devious, non-business purposes.

Courts, however, have trouble applying the CFAA's vague "authorization" language to the delicate and complex relationship that exists between employees and employers. Naturally questions arise over what it means to access without authorization or exceed authorized access when the person's employee status means that he already has authorization to access a computer—that is, his employer has directed him to use a computer and create, modify, or otherwise use the information on that computer system. In response to the problem of applying the CFAA's vague statutory language in employment situations, courts have developed three different understandings of authorization: agency based, code based, or contract based. Courts following an agency-based interpretation determine authorization through principles of agency law, such as employee loyalty.[5] Courts opting for a code-based interpretation define authorization by technical limits within computer systems, such as employer-installed password requirements.[6] Finally, some courts apply a contract-based interpretation under which authorization is determined by contractual limits placed in employee agreements and policies.[7]

The current state of confusion over how to define an employee's liability for computer misuse under the CFAA is undoubtedly less than ideal. This Note seeks to provide some clarity to the dispute by analyzing the legislative history and asking which approach best effectuates legislative intent behind the CFAA. Ultimately this Note suggests that courts should adopt a code-based approach to authorization as a default interpretation, while allowing contracts that are clearly applicable and aimed to prevent computer misuse to define authorization in some CFAA employment cases. Part I reviews the various interpretations of authorization within the employment context. Part II analyzes the legislative history of the CFAA, noting that while this history does not supply meaningful information regarding the specific legislative intent behind the authorized-access phrases within the CFAA, a more general look at the legislative history provides two valuable insights: first, the general legislative aim of the CFAA is combating computer misuse; and second, there is congressional assent to greater judicial discretion

---

5. *See, e.g.*, Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006); ViChip Corp. v. Lee, 438 F. Supp. 2d 1087, 1100 (N.D. Cal. 2006); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).

6. *See, e.g.*, Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 968 (D. Ariz. 2008); Diamond Power Int'l., Inc. v. Davidson, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007); Lockheed Martin Corp. v. Speed, No. 6:05-cv–1580–Orl–31KRS, 2006 U.S. Dist. LEXIS 53108, at *15 (M.D. Fla. Aug. 1, 2006).

7. *See, e.g.*, Modis, Inc. v. Bardelli, 531 F. Supp. 2d 314, 319 (D. Conn. 2008); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 498 (D. Md. 2005); SecureInfo Corp. v. Telos Corp., 387 F. Supp. 2d 593, 608–10 (E.D. Va. 2005).

in defining authorization in CFAA cases involving insiders, such as employment cases. Based on these insights, Part III proposes the adoption of a code-based default interpretation and evaluates the merits of the agency-based approach and the contract-based approach as alternative interpretations in CFAA employment cases. This Part concludes by stressing the value of an approach where courts prefer a code-based understanding of authorization in most situations, but are free to deviate and determine authorization based on contracts in certain CFAA employment cases.

I. THREE INTERPRETATIONS OF AUTHORIZATION

Although the CFAA is primarily a criminal statute, individuals and companies can also bring private civil suits against CFAA violators.[8] Many of these civil suits involve employers and their former employees.[9] In such suits, the employing company uses the CFAA to receive damages or an injunction after an employee uses a company computer to access, email, or copy sensitive company information.[10] A company's success in proving a violation of the CFAA within a given set of facts often turns on the court's answer to the following question: what does it mean to say that a person "intentionally accesses a computer without authorization or exceeds authorized access"?[11] The ambiguity of the statutory language has led courts to adopt different approaches to answering this question, with the result that employers and employees are often left without a consistent understanding of how a court will assess their CFAA claims.

One can, however, distill three distinct categories of approaches from the courts' treatment of authorization in CFAA employment cases: the agency-based interpretation, the code-based interpretation, and the contract-based interpretation of authorization. These different interpretations have emerged slowly; it was only recently, after the Seventh Circuit's endorsement of an agency-based approach, that courts began to expressly note the possibility of alternative interpretations to authorization in their opinions.[12] This Part

---

8. 18 U.S.C. § 1030(g) (allowing any person who suffers damage by a violation of the CFAA to "maintain a civil action" for "compensatory damages and injunctive relief or other equitable relief").

9. Civil suits under the CFAA have also been brought by website operators against users of electronic data gatherers, Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 322–23 (2004), and by internet service providers against spammers, Saul Hansell, *Microsoft Sues 15 Organizations In Broad Attack On Spam E-Mail*, N.Y. TIMES, June 18, 2003, at C1.

10. *See* Paul S. Chan & John K. Rubiner, *Access Denied: Using the Computer Fraud and Abuse Act to Restrict Employee Mobility*, COMP. & INTERNET LAW., June 2006, at 12, 12–14.

11. 18 U.S.C. § 1030(a)(2).

12. *Compare* United States v. Czubinski, 106 F.3d 1069, 1071–72 (1st Cir. 1997) (finding access unauthorized without discussing how to determine authorization), United States v. Morris, 928 F.2d 504, 510–11 (2d Cir. 1991) (finding that lack of authorization is not limited to outsiders, but not discussing alternative interpretations of authorization), and Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000) (applying an agency-based interpretation of authorization without noting alternatives), *with* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 964–65 (D. Ariz. 2008) (noting the existence of different interpretations),

explores the development and operation of each of the categories of interpretation of employees' authorization in CFAA cases.

A. *Agency-Based Interpretation*

As suggested by the name, the agency-based interpretation of authorization is based on common-law agency principles.[13] The employer-employee agency relationship imposes "special duties on the part of both the employer and the employee which are not present in the performance of other types of contracts."[14] Important for our concerns, the employee owes a duty of loyalty to his employer, which requires him to act solely for the benefit of the employer or company.[15] Moreover, the employee's authority to act on behalf of the employer terminates when he obtains an interest adverse to the employer—for example, if he begins to work for a competitor.[16] Thus, importing these principles into authorization under the CFAA, an employee's authorization is implicitly revoked when he accesses a computer for purposes that do not further his employer's interests.

Courts adopting the agency-based interpretation determine whether computer access was authorized under the CFAA through the direct use of these basic agency principles. In the first case to apply agency principles, an employee of a self-storage business emailed confidential information to a competitor just prior to leaving to work for that competitor.[17] In determining whether this access was unauthorized and violated the CFAA, the court relied on section 112 of the Second Restatement of Agency, which states, "Unless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[18] Applying this principle, the court found that "the authority of the plaintiff's former employee[] ended when [he] allegedly became [an] agent[] of the defendant . . . when [he] allegedly obtained and sent the proprietary information to the defendant via e-mail."[19] Notably, the court claimed that this agency-based interpretation was the plain meaning of authorization within the CFAA and in line with its legislative history.[20]

Black & Decker (U.S.), Inc. v. Smith, 568 F. Supp. 2d 929, 933–34 (W.D. Tenn. 2008), *interlocutory appeal granted*, No. 07–1201, 2008 WL 3850825 (W.D. Tenn. Aug. 13, 2008) (same), and Lockheed Martin Corp. v. Speed, No. 6:05–cv–1580–Orl–31KRS, 2006 U.S. Dist. LEXIS 53108, at *12–14 (M.D. Fla. Aug. 1, 2006) (same).

13. *See, e.g.*, *Shurgard*, 119 F. Supp. 2d at 1125.

14. WILLIAM A. GREGORY, THE LAW OF AGENCY AND PARTNERSHIP 10–11 (3d ed. 2001).

15. *Id.* at 13.

16. RESTATEMENT (SECOND) OF AGENCY § 112 (1958); GREGORY, *supra* note 14, at 103.

17. *Shurgard*, 119 F. Supp. 2d at 1123.

18. RESTATEMENT (SECOND) OF AGENCY § 112.

19. *Shurgard*, 119 F. Supp. 2d at 1125.

20. *Id.* at 1129.

The Seventh Circuit gave credit to this interpretation by adopting it in *International Airport Centers, L.L.C. v. Citrin*.[21] There, the court used agency principles to find that an employee violated the CFAA by deleting all the data on a company laptop and loading a secure-erasure program to ensure that none of the deleted information was recoverable.[22] The court relied on agency law in assessing Citrin's actions:

> [Citrin's] authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit IAC in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee.[23]

Although the Seventh Circuit's decision also cited section 112 of the Second Restatement of Agency, the court focused more broadly on the duty of loyalty concept within agency law.[24] The court noted that the only basis of Citrin's authority to access the laptop rested in his agency relationship with IAC and that the agency relationship ended when Citrin breached his duty of loyalty.[25]

The import of the Seventh Circuit's decision to adopt the agency-based interpretation in *Citrin* has been notable. The decision has acted as a validation of that approach for many judges, as the number of district courts now employing an agency-law understanding of authorization in determining CFAA claims suggests.[26] Additionally, practitioners have taken note of the decision, releasing papers on how to both use this interpretation of the CFAA to one's advantage[27] and mitigate its negative implications.[28] Notable as well is the fact that this agency-based interpretation is undoubtedly the most employer-favorable approach, since simply characterizing the employee's actions as against the employer's interests will likely result in liability.[29] Indeed, while there is no compiled data for the assertion, the acceptance of this approach by a major circuit court appears to have increased company filings of CFAA claims.[30] Since *Citrin*, it has become clear that the agency-based interpretation is beginning to become a real contender as the

---

21. 440 F.3d 418 (7th Cir. 2006).

22. *Id.* at 419.

23. *Id.* at 420.

24. *Id.* at 420–21.

25. *Id.*

26. *See, e.g.*, ViChip Corp. v. Lee, 438 F. Supp. 2d 1087, 1100 (N.D. Cal. 2006).

27. *See, e.g.*, Richard Warner, *The Employer's New Weapon: Employee Liability Under the Computer Fraud and Abuse Act*, 12 EMP. RTS. & EMP. POL'Y J. 11, 12, 23 (2008).

28. *See, e.g.*, Chan & Rubiner, *supra* note 10, at 16.

29. *Id.* at 14.

30. Shepardizing the opinion establishes that thirty-one cases have cited *Citrin* since the decision was issued in March 2006. Opinion last Shepardized using LexisNexis on December 5, 2008.

leading interpretation of authorization within the CFAA. Yet the costs of this approach may outweigh its benefits.[31]

B. *Code-Based Interpretation*

The code-based interpretation of authorization is rooted in the operation of computer systems; access is unauthorized where a person bypasses code-based protections designed to limit his use of the computer system.[32] This can occur where an individual guesses at passwords or uses other false means to get past a password-protected zone or other security mechanism.[33] Notably, this understanding of authorization limits liability to instances where a user explicitly manipulates a computer system into giving him greater access and use privileges than he would otherwise have.[34] As such, where an employee has been affirmatively granted the ability to use and access a computer database or system, his authorization cannot be challenged under the code-based interpretation.[35]

The code-based interpretation can be traced back to the earliest CFAA cases involving authorization questions. For example, *United States v. Morris*[36] invoked a close analogue to the code-based interpretation with its "intended function" test.[37] In *Morris*, the Second Circuit held that a graduate student violated the CFAA by accessing computers without authorization because he used email and other programs in a manner not related to their intended function; his use instead located holes in the programs, giving him a special and unauthorized access route into other computers.[38] Thus, the intended function test asks whether a user violated the intended function of a network or program to gain access not intended by the programmer or network administrator.[39] The test is similar to a code-based interpretation of authorization because violation of the intended function is often done through technical means, such as by finding holes in programs, or bypassing passwords or other protection systems.[40]

---

31. *See infra* Section III.B.1.

32. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1600 (2003).

33. *Id.* at 1644–45.

34. *Id.* at 1649.

35. *See, e.g.*, Black & Decker (U.S.), Inc. v. Smith, 568 F. Supp. 2d 929 (W.D. Tenn. 2008), *interlocutory appeal granted*, No. 07–1201, 2008 WL 3850825 (W.D. Tenn. Aug. 13, 2008).

36. 928 F.2d 504 (2d Cir. 1991).

37. Kerr, *supra* note 32, at 1649.

38. *Morris*, 928 F.2d at 510.

39. Kerr, *supra* note 32, at 1632.

40. Notably, the intended function test can be somewhat broader than a code-based interpretation of authorization, as other courts have interpreted it to mean that the scope of a user's authorization derives from the expected norms of intended use or the nature of the relationship established between the computer owner and the user. United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007). However, the operation of the intended functions test in the *Morris* case specifically

More recently, courts have revived the code-based interpretation of authorization in CFAA cases involving employees and employers as a response to the agency approach used in *Shurgard* and *Citrin*. Perhaps the most vocal criticism of the use of agency principles in *Citrin* came in a district court opinion from Florida, *Lockheed Martin Corp. v. Speed*.[41] The circumstances in *Speed* were factually similar to those in *Shurgard*. Plaintiff Lockheed Martin claimed that competitor L-3 conspired with three of Lockheed's former employees to wrongfully obtain trade secrets.[42] The court noted that the plain language of the statute was sufficiently clear such that courts should not resort to extrinsic materials like the Second Restatement of Agency, as done in *Shurgard* and *Citrin*.[43] Moreover, the court asserted that the use of agency principles created an inconsistency within the text of the CFAA.[44] Finally, the court concluded that reading agency principles into authorization would bring "remarkable reach to the statute" and pose problems in the criminal context with regard to the rule of lenity.[45]

A close reading of *Speed* demonstrates that the court favored a more code-based interpretation of authorization, which it labeled as the "plain language" interpretation of authorization.[46] Under this interpretation, the court found that because the employees were permitted to access the company computers and the precise information at issue, they were not acting without authorization or exceeding authorized access.[47] The court explicitly noted that the CFAA only concerns itself with improper access and not what the employees may have done with information after authorized access.[48] In evaluating the technical authority of the individuals to access—looking only at whether an employee has exceeded the level of access they have been granted by employers and not at the motive behind the questioned access—the *Speed* court's plain language interpretation of authorization is more properly labeled as code based.

In the few years since the *Speed* decision first challenged the agency-based interpretation adopted by the Seventh Circuit, other district courts

---

translates into a code-based approach of authorization, because Morris used holes in programs to allow himself greater access than he would otherwise have had. *Morris*, 928 F.2d at 510.

41. No. 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at *16–25 (M.D. Fla. Aug. 1, 2006).

42. *Id.* at *3.

43. *Id.* at *12.

44. The court noted that the use of agency principles to determine that an employee was "without authorization" suggests that the term "exceeds authorized access" should not apply to situations involving a person with some level of authorization (i.e., insiders). *Id.* at *18–19. As such, the court concluded, the agency-based interpretation "effectively shaves 'exceeds authorized access' down to a mere sliver of what its plain meaning suggests." *Id.* at *17.

45. *Id.* at *22–23.

46. *See id.* at *15.

47. *Id.* at *15.

48. *Id.* at *15–16.

have similarly expressed hesitancy about the *Citrin* approach.[49] Like the *Speed* court, these courts place significance on the fact that individuals have been expressly allowed to view or use information, finding it irrelevant with regard to liability under the CFAA whether the ultimate use of that information was improper in the employment context.[50] Although a circuit court has not yet explicitly adopted the code-based interpretation of authorization, these district court decisions challenge the agency-based approach. Moreover, this competing approach—the code-based interpretation of authorization—is notably less employer-friendly, because the employee's access in these employment-related CFAA cases is usually clearly authorized in the code-based understanding of that term.[51]

C. *Contract-Based Interpretation*

The contract-based interpretation requires the computer user to violate a contract before that user's access can be found to be unauthorized.[52] This requires then the existence of an explicit or implicit contract that defines the authorization of a particular user. As such, this interpretation is often invoked in cases involving internet or website providers where there is a contract or terms-of-service agreement between the parties[53] or cases between former employers and employees where there is an employment contract or handbook.[54] In employment cases, these contracts could take a variety of forms, from confidentiality agreements to employee handbooks, and courts are just beginning to examine the language necessary to determine authorization for CFAA purposes.

A few cases have explored which types of documents can serve as the contractual basis for determining authorization in employment cases. In two

---

49. *See, e.g.*, Black & Decker (U.S.), Inc. v. Smith, 568 F. Supp. 2d 929 (W.D. Tenn. 2008), *interlocutory appeal granted*, No. 07–1201, 2008 WL 3850825 (W.D. Tenn. Aug. 13, 2008); B&B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007).

50. *See, e.g.*, *Black & Decker*, 568 F. Supp. 2d at 936; Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 968 (D. Ariz. 2008); Brett Senior & Assocs. v. Fitzgerald, No. 06–1412, 2007 WL 2043377, at *3 (E.D. Pa. July 13, 2007); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 494–98 (D. Md. 2005); SecureInfo Corp. v. Telos Corp., 387 F. Supp. 2d 593, 608–10 (E.D. Va. 2005).

51. *See, e.g.*, *Shamrock Foods*, 535 F. Supp. 2d at 968.

52. Kerr, *supra* note 32, at 1637.

53. *See, e.g.*, Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 448 (E.D. Va. 1998) (finding that use of an AOL account to obtain email addresses of other users constituted unauthorized access of information because it violated AOL's terms of service). Courts have varied in their acceptance of the contract-based interpretation of authorization. Some courts hesitate in using terms of service agreements to determine authorization. *See* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000). However, other courts have found unauthorized access using a contract-based interpretation even when the access was not specifically prohibited by the contract. *See* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248 (S.D.N.Y. 2000).

54. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001); United States v. Czubinski, 106 F.3d 1069, 1071 (1st Cir. 1997); Modis, Inc. v. Bardelli, 531 F. Supp. 2d 314, 319 (D. Conn. 2008); Hewlett-Packard Co. v. Byd:Sign, Inc., No. 6:05–CV–456, 2007 WL 275476, at *15 (E.D. Tex. Jan. 25, 2007).

related cases, the First Circuit determined that a competitor and several former employees had " 'exceed[ed] authorized access' "[55] in using a scraper[56] to get large amounts of data regarding pricing off the website of EF, a tour guide company.[57] The court found such a violation of the CFAA after determining that the former employees exceeded the bounds of a confidentiality agreement that they had with their former employer.[58] The First Circuit also explicitly noted the need for contracts to clearly outline the limits of authorization for liability to stick under a contract-based interpretation.[59]

Employee handbooks and rules have similarly provided the foundation for a contract-based interpretation of authorization. In *United States v. Czubinski*, the First Circuit focused on an IRS employee's signed acknowledgement of receipt of the IRS Rules of Conduct limiting computer-system use to official purposes as well as separate rules relating to a specific database that limited access to "only those accounts required to accomplish your official duties."[60] Based on these contracts, the court determined that by browsing the tax returns of acquaintances, the employee had "unquestionably exceeded authorized access" under the CFAA.[61] This language from the opinion suggests that employers can contractually define the limits of authority and that courts may use these contracts to conclude whether an employee has exceeded his authority under the CFAA.[62]

Language within employment contracts and documents can vary greatly, with some having only vague reference to employees maintaining confidentiality and not exposing trade secrets, and others explicitly stating that employees are not authorized to access or distribute certain confidential company information. Some courts using the contract-based interpretation have been firm in requiring contracts to be on the latter side of the specificity spectrum—to explicitly state the limits of employees' authorization.[63] In *Hewlett-Packard Co. v. Byd:Sign, Inc.*, a district court used confidentiality agreements and an employer's "Standards of Business Conduct" document to evaluate the plaintiff's claims that employees lacked authority to access

---

55. EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003) (quoting 18 U.S.C. § 1030(e)(6) (2006)) (alteration in original); *Explorica*, 274 F.3d at 581 (quoting 18 U.S.C. § 1030(e)(6) (2006)) (alteration in original).

56. Scrapers are computer programs that are able to quickly gather all the information on a website. *Explorica*, 274 F.3d at 579.

57. *Zefer*, 318 F.3d at 62–63; *Explorica*, 274 F.3d at 579.

58. *Explorica*, 274 F.3d at 583. In *Zefer*, the court noted that the lack of authorization also implicitly extended to Zefer, the company that created the scraper, even though it was not a party to the confidentiality agreement. 318 F.3d at 63.

59. *Id.* at 63–64. The court noted that "[i]t is also of some use for future litigation among other litigants in this circuit to indicate that, with rare exceptions, public website providers ought to say just what non-password protected access they purport to forbid." *Id.* at 64.

60. 106 F.3d 1069, 1071 (1st Cir. 1997).

61. *Id.* at 1078.

62. Kerr, *supra* note 32, at 1634.

63. Hewlett-Packard Co. v. Byd:Sign, Inc., No. 6:05–CV–456, 2007 WL 275476, at *12 (E.D. Tex. Jan. 25, 2007).

confidential information in order to send it to a competing enterprise that they had established.[64] The court noted a factual difference from other cases where employees were found not to have exceeded authorized access.[65] Specifically, the court stated that the employees in the other cases were authorized to access the information at issue and the complaints were more about what the employees did with the information once obtained.[66] In contrast, the HP employees had agreed both to not disclose information and "to refrain from sending or accessing messages on HP's computer systems for personal gain."[67] Since their activities included this accessing and transferring, the court noted that HP successfully alleged the employees exceeded their authorization as defined in the employment agreements.[68] Thus, a stricter contract-based interpretation of authorization may require the employment contract to explicitly ban the use of a computer in certain activities the company defines as unauthorized.

The contract-based-approach requirement of an actual contract or agreement capable of being interpreted as defining an employee's authorization, as well as the lack of developed case law on how specifically applicable such an agreement needs to be, means that these cases are somewhat on the periphery of the debate over the proper approach to authorization in CFAA employment cases.[69] Nonetheless, because employment situations often do involve such contracts and agreements, this approach has the potential for real legitimacy in CFAA employment cases, even if happens to be underappreciated by courts within the broader debate.

II. LEGISLATIVE HINTS

With rather ambiguous language such as "accesses . . . without authorization, or exceeds authorized access,"[70] the CFAA is, unsurprisingly, not interpreted and applied in any consistent manner. Seeking additional information to inform their decisions, many of the courts struggling to interpret authorization have turned to the CFAA's legislative history, often finding

64. *Id.* at *1.

65. *Id.* at *13.

66. *Id.*

67. *Id.*; *see also* Modis, Inc. v. Bardelli, 531 F. Supp. 2d 314, 319 (D. Conn. 2008) (noting that the employee's authorization was limited to access in furtherance of the employer's business based on language in an employment agreement).

68. *Hewlett-Packard*, 2007 WL 275476, at *13.

69. Indeed, most cases following *Citrin* and *Speed* that outline the conflict between an agency-based approach and a code-based approach fail to mention the possibility of a contract-based approach entirely, even when there exists a contract capable of being interpreted as defining authorization. *See, e.g.*, Black & Decker (U.S.), Inc. v. Smith, 568 F. Supp. 2d 929, 934–36 (W.D. Tenn. 2008), *interlocutory appeal granted*, No. 07–1201, 2008 WL 3850825 (W.D. Tenn. Aug. 13, 2008) (outlining the divide between courts applying an agency-based approach and those applying a code-based approach and adopting the latter without substantial consideration of the employment agreements relating to the employee's authorization).

70. 18 U.S.C. § 1030(a)(4) (2006).

support for whichever interpretation they themselves adopt in the end.[71] This Part reviews the legislative history removed from any factual considerations that may have colored these courts' analyses. It seeks to determine what, if any, value and insight can be derived from such history, with the analysis loosely informed by three values that legislative history might serve: authority, purpose, and truth.[72] Section II.A evaluates whether the legislative history provides any authority value in terms of explaining the legislature's specific intent as to the meaning of authorization and insider access. This Section concludes that because the legislative history contains independent support for each approach, no single approach is justified on the grounds that it represents the congressionally dictated interpretation of authorization. Section II.B takes a broader approach to the CFAA's legislative history, seeking to uncover the statutory purpose and any legislative assumptions regarding its operation. Evaluating the general intent or purpose of the CFAA, Section II.B.1 finds that the legislative aim of the CFAA was to create liability for computer misuse and that the code-based approach best approximates this aim. Section II.B.2 focuses on a particular insight that emerges from a more generalized and contextual evaluation of the legislative history—one that lends support to allowing some judicial discretion in the interpretation of authorization in employment cases.

A. *Specific Legislative Intent or the Lack Thereof*

Courts struggling with statutory interpretation often turn to the legislative history to determine exactly what Congress meant when it used a particular word or phrase.[73] Searching the legislative history to ascertain the intention of Congress when referring to "authorized access" and, specifically, how it intended authorization to be determined in insider situations,[74] this Section determines that the legislative history does not support a legislative preference for any one of the three approaches above the others.

---

71. Courts opting for an agency-based interpretation use legislative history to find that the CFAA's scope has been broadened over time such that it reaches and can be invoked by employers and that the CFAA was designed to reach insiders as well as outsiders. *See, e.g.*, Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127–29 (W.D. Wash. 2000); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 417 (7th Cir. 2006). Courts adopting a code-based interpretation often argue that the legislative history supports a narrow view of authorization. *See, e.g.*, Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965–66 (D. Ariz. 2008).

72. William N. Eskridge, Jr., *Legislative History Values*, 66 CHI.-KENT L. REV. 365, 439 (1990).

73. Use of legislative history is declining generally, but many courts still employ it where the statutory text is ambiguous. CHRISTIAN E. MAMMEN, USING LEGISLATIVE HISTORY IN AMERICAN STATUTORY INTERPRETATION 26 (2002). Using legislative history as evidence of specific intent, as I do here, "is, historically, the main justification for examining such materials." Eskridge, *supra* note 72, at 369–70.

74. Initially, the CFAA was primarily aimed at outsiders, such as hackers or other persons outside of the computer system at issue. *See* H.R. REP. No. 98–894, at 10–12 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695–97. Insiders, by contrast, are those who are somehow legitimately connected to the computer system at issue. In employment-related CFAA cases, issues of insider liability acquire acute importance, because employees are generally considered insiders in light of their employer-sanctioned access.

Because evidence of Congress's specific intent with respect to authorization in the CFAA can be characterized as supporting each of the three interpretations commonly asserted by courts in some form, the legislative history provides little authority value to the current debate.

A court seeking to use legislative history to determine which understanding of "authorization" Congress intended would do well to focus on the congressional discussion of insider liability under the CFAA. Much of the original 1984 statute focused on criminalizing computer misuse by outsiders—"hackers" and individuals using computers to "to break into other computer systems."[75] However, the statute's reach was not limited to just those without authorization; it extended to anyone who "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend."[76] In later amendments to the statute, Congress repeatedly mentioned this insider liability, particularly in reference to a desire that insiders not face high liability under the statute.[77]

Congress's initial discussion of the limits of any insider liability in the statute suggests an understanding that insider authorization is determined by the *purpose* of the access—an understanding that arguably aligns with either the agency-based approach adopted by courts (where valid or invalid purposes are defined through agency principles) or the contract-based approach (where valid or invalid purposes are defined in contract terms). In discussing the meaning of the original "exceeds authorized access" provision, the House Committee noted that it did not want to extend the 1984 Act "to any type or form of computer access that is for a legitimate business purpose. Thus, any access for a legitimate purpose that is pursuant to an express or implied authorization would not be affected."[78] Although this statement sought to define a limit to insider liability, the lack of a definition or explanation of "legitimate purposes" left confusion as to the borders of that limited liability.[79] Moreover, Congress included other phrases in the 1984 Act to ensure that insiders engaged in nonharmful, but perhaps not fully legitimate, activities, such as using a computer for computer games, were not criminally liable.[80] The clarification that an insider does not overreach his authorized access to a computer by using it for legitimate purposes or even nonharmful, illegitimate purposes suggests that Congress originally

---

75. H.R. REP. No. 98–894, at 10, *reprinted in* 1984 U.S.C.C.A.N. at 3695.

76. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98–473, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2006)) [hereinafter 1984 CFAA].

77. *See* S. REP. No. 104-357, at 11 (1996); H.R. REP. No. 99-612, at 7, 10–11 (1986); S. REP. No. 99-432, at 5–7 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2483–85.

78. H.R. REP. No. 98-894, at 21, *reprinted in* 1984 U.S.C.C.A.N. at 3707.

79. Joseph B. Tompkins, Jr. & Linda A. Mar, *The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem*, 6 COMPUTER/L.J. 459, 465 (1986).

80. H.R. REP. No. 98-894, at 15, 22, *reprinted in* 1984 U.S.C.C.A.N. at 3701, 3708 ("[The 1984 Act] adds a clause excluding from these sections coverage of a person authorized to access a computer who merely exceeds such authorization by the incidental use of the computer . . . . in, for example, doing one's homework or playing computer games.").

understood insider authorization to be determined either by the limits defined to them by their employers or general norms of use.[81] Thus, it appears that this original understanding was more on par with agency-based or contract-based interpretations later used by courts than the code-based interpretations.

Congressional commentary about some of the alterations to the statute suggests that Congress maintained this particular understanding of insider authorization through the 1986 amendments. Specifically, the maintenance of a legitimate purpose understanding is alluded to in congressional discussion relating to the modification of the section covering trespass to government computers in § 1030(a)(3) in conjunction with the addition of the section covering a wider range of computers, but requiring a specific intent to defraud, in § 1030(a)(4). To address complaints that the 1984 Act would have a "chilling effect" on government whistleblowers, Congress removed the "exceeds authorized access" equivalent provision from § 1030(a)(3).[82] The House Committee report noted that absent such a change, this provision would mean that the section covered "[t]he improper modifications, destructions or disclosures by authorized users of Federal computers."[83] Focusing on the "improper" nature of the access, this comment suggests a view of authorization consistent with that expressed in the reports on the 1984 Act, where authorization was contingent on "legitimate purposes." Additionally, in discussing the elimination of the authorized user provision from § 1030(a)(3), Congress noted that such improper insider activities were still subject to the new "intend to defraud" felony offense in § 1030(a)(4).[84] Thus, the discussion regarding the changes to § 1030(a)(3) suggests that Congress did not change its understanding that authorization was governed by acceptable purposes, although how these purposes were known to insiders remained vague.

By focusing on the purposes behind an insider's access, the above recitation could be used to find congressional intent for either an agency-based or a contract-based approach to authorization in employment situations. Since these discussions of legitimate purposes are somewhat vague in the legislative history, the agency-based approach and its similarly nebulous concept of loyalty is arguably better supported. However, since an employment contract could easily categorize the legitimate purposes that define an insider's authorized access, the contract-based approach could also receive some corroboration in light of the legislative history outlined above.

In addition to support for an agency- or contract-based approach, the legislative history could be used to simply argue against a code-based approach with respect to insider authorization. In discussing other 1986

81. *See* Tompkins & Mar, *supra* note 79, at 465.

82. H.R. REP. No. 99-612, at 7.

83. *Id.*

84. *Id.*

changes to the law meant to protect insiders from overly harsh penalties,[85] Congress continued to express an understanding of insider authorization governed by something other than code-based restrictions. The Senate Committee report criticized the old "knowingly" standard:

> [T]his standard might not be sufficient to preclude liability on the part of those who inadvertently "stumble into" someone else's computer file or computer data. This is particularly true in those cases where an individual is authorized to sign onto and use a particular computer, but subsequently exceeds his authorized access by mistakenly entering another computer file or data that happens to be accessible from the same terminal. . . . The substitution of an "intentional" standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another.[86]

If Congress intended to apply a purely code-based understanding of authorization to insiders, it likely would not have this concern about mistaken employees being prosecuted for stumbling into computer files that they were not allowed to access. Presumably, the mere fact that these files were not password protected or encrypted and were accessible to the employee would mean that employees were not exceeding their authorization by accessing them.

Yet just as an argument could be made against a code-based approach, there is fodder within the legislative history to discount the other two approaches as well and, perhaps, provide a bit of support to the code-based approach. Specifically, the legislative history to the 1986 amendments provides two instances suggesting that Congress could have intended something other than an agency-based or contract-based approach to authorization.

First, the congressional report states that insiders accessing computers of other departments of the government are "without authorization" and therefore liable under § 1030(a)(3).[87] While such limits on interdepartmental access could be defined through either agency norms or contracts, presumably, these limits could also take the form of code-based measures preventing access to computers in other departments. By failing to explain what specifically makes the insider's access unauthorized in this situation, the legislative history introduces this further doubt into how Congress intended employee authorization to be determined.

In addition, under the 1984 Act, a user faced civil liability only if he intentionally accessed a computer (1) "without authorization" or (2) "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend."[88] The

---

85. *Id.* at 7, 10–11; SEN. REP. No. 99-432, at 5–7 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2482–85.

86. S. REP. No. 99-432, at 6, *reprinted in* 1986 U.S.C.C.A.N. at 2483–84.

87. S. REP. No. 99-432, at 8, *reprinted in* 1986 U.S.C.C.A.N. at 2486.

88. 1984 CFAA, *supra* note 76.

1986 amendments, however, replaced this second phrase with "exceeds authorized access," defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[89] Although the committee reports state that this change is merely to simplify the statute's language,[90] the language in the definition of "exceeds authorized access" is notably different than that in the 1984 Act's insider authorization clause.[91] Instead of determining authorization by focusing on purposes, the 1986 version looks to one's entitlement to information or data.[92] This change may be understood as a move by Congress to get away from the confusion created by the 1984 Act with regard to "legitimate purposes." However, the "exceeding authorized access" language and definition do not help clarify when insider access is unauthorized. Specifically, this amendment merely shifts the focus to insider's entitlement to information or data and fails to explain whether such entitlement is determined by code-based limits to one's ability to access or by employer-defined limits.[93]

Regardless of any criticism of the use of legislative history to give authoritative content to statutory language,[94] the review of the legislative history here suggests that, at least on the question of what Congress specifically intended "unauthorized access" to entail in employment (i.e., insider) situations, legislative history does not unambiguously support, and thus provides little authority value to, any of the three interpretations offered by courts.

B. *Looking More Broadly: The General Legislative Aim of Combating Computer Misuse and an Allowance of Judicial Discretion*

Although evidence of a congressional intent for any specific interpretation of "unauthorized access" may be lacking, legislative history may still inform the debate. Specifically, it can serve as a source of contextual information that can aid in determining which approach to "unauthorized access"

---

89. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213, § 2(g)(6) (codified as amended at 18 U.S.C. § 1030 (2006)) [hereinafter 1986 CFAA].

90. S. REP. No. 99-432, at 9, *reprinted in* 1986 U.S.C.C.A.N. at 2486; H.R. REP. No. 99-612, at 11.

91. *See* 1984 CFAA, *supra* note 76, at § 2102(a).

92. *See* 18 U.S.C. § 1030(e)(6).

93. Further amendments to the CFAA do not provide any more information about what Congress intended to determine insider authority. The most significant amendments to the CFAA after 1986 reference insider unauthorized users multiple times, but primarily to explain that provisions do reach insiders exceeding their authorized access. *See* S. REP. No. 104-357, at 6, 9–11 (1996). The later committee reports on the CFAA again make it clear that Congress wants to include insiders who are exceeding their authorized access purposefully and with an intent to harm, but these discussions fail to clarify what insider actions cause a person to exceed authorization. *See id.* at 11; S. REP. No. 101-544, at 5 (1990).

94. *See, e.g.*, Wis. Pub. Intervenor v. Mortier, 501 U.S. 597, 622 (1991) (Scalia, J., concurring) (objecting to "the practice of utilizing legislative history for the purpose of giving authoritative content to the meaning of a statutory text").

should prevail in CFAA employment cases.[95] An examination of the legislative history from this broader perspective establishes that Congress specifically intended the CFAA to create liability for instances of computer misuse—that is, behavior that is criminal because it misuses a computer—and not the broader category of traditional criminal behavior facilitated by the use of a computer. Explored in Section II.B.1, this general purpose of the CFAA suggests that a code-based approach is the best default interpretation of authorization. But a broader look at the legislative history also furnishes a second insight, which is discussed in Section II.B.2; this insight provides that courts may, in their discretion, choose the interpretation of authorization they deem most appropriate in CFAA cases involving insiders.

1. *The General Legislative Aim of Combating Computer Misuse*

A more generalized view of the CFAA's legislative history, specifically in terms of its purpose value, establishes that the CFAA is inherently aimed at curbing crimes of computer misuse. Crimes using computers can be divided into two types: traditional crimes using computers and crimes of computer misuse.[96] Professor Kerr best describes the difference between the two, noting that the former "involve the online commission or facilitation of traditional criminal offenses" such as "Internet fraud schemes, Internet gambling, online distribution of child pornography, and cyberstalking."[97] Notably, although the incidence of this type of computer crime increased as computers became more widely used, it remains susceptible to prosecution under traditional criminal offenses and, thus, required no significant development of the law.[98]

In contrast, computer-misuse crimes involve "conduct that intentionally, knowingly, recklessly, or negligently causes interference with the proper functioning of computers and computer networks."[99] Kerr provides examples such as "computer hacking, distribution of computer worms and viruses, and denial-of-service attacks."[100] This latter type of computer crime, crimes of computer misuse, presented serious new problems for criminal law in the late 1970s and early 1980s.[101] Traditional offenses, like trespass and burglary, while arguably applicable, posed insurmountable conceptual

95. *See* MAMMEN, *supra* note 73, at 156; *see also* Adam N. Steinman, *"Less" is "More"? Textualism, Intentionalism, and a Better Solution to the Class Action Fairness Act's Appellate Deadline Riddle*, 92 IOWA L. REV. 1183, 1218 (2007) ("Both textualists and intentionalists agree that statutory language can be ambiguous, and in those situations, it is proper for judges to consult not only the statute's text but also its context, including the legislative intent underlying that statute.").

96. Kerr, *supra* note 32, at 1602.

97. *Id.* at 1602–03.

98. *Id.* at 1603.

99. *Id.*

100. *Id.* at 1603–04.

101. *Id.* at 1603–05.

problems.[102] And while theft law was often used to prosecute computer misuse, courts were initially hesitant to characterize computer misuse as the taking of property,[103] although some soon adopted creative understandings of property to find that computer information was subject to theft laws.[104] Having some courts manipulate traditional doctrines while others found no recourse for punishing computer misuse was not ideal,[105] and this uncomfortable fit between the computer-misuse crimes and traditional criminal law doctrines triggered calls for computer-crime legislation in the late 1970s and early 1980s.[106] Thus, the CFAA was originally conceived as a specific response to the growing concern of computer-misuse crimes rather than traditional crimes using computers.[107] This conception of the CFAA as a tool to prosecute crimes of computer misuse can also be seen in later amendments to the statute that specifically target emerging computer-misuse crimes rather than traditional crimes accomplished by using computers.[108]

Awareness of this general legislative intent of the CFAA can inform the debate over which approach courts should take in interpreting authorization in employment cases. Specifically, it suggests that any approach taken should be consistent with the idea that the CFAA seeks to capture crimes of computer misuse rather than traditional offenses using a computer.[109]

A code-based approach clearly meets the general purpose of targeting only crimes of computer misuse. Under a code-based interpretation, authorization is determined by whether the codes that constrain one's access to a computer or particular files have been circumvented, either by falsely using another's privileges or taking advantage of weaknesses in the computer's

---

102. *Id.* at 1605–07 (noting that trespass and burglary statutes require physical entry onto property, which one cannot do in cyberspace); Joseph M. Olivenbaum, *<CTRL><ALT><DEL>: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 577 (1997) (same with regard to trespass and larceny).

103. *See, e.g.*, Lund v. Commonwealth, 232 S.E.2d 745, 748 (Va. 1977) (stating that unauthorized use of a computer is not subject to the larceny statute).

104. *E.g.*, United States v. Girard, 601 F.2d 69, 71 (2d Cir. 1979) (concluding that the government has a property interest in information); United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978) (finding that the defendant's unauthorized use and accessing of computerized information was akin to being an intruder on the physical property of another).

105. As Kerr notes, even those courts willing to find that a crime had been committed by computer misuse often only punished computer misuse as theft when it resulted in significant harm. Kerr, *supra* note 32, at 1613.

106. *Id.*; *see also* DONN B. PARKER, FIGHTING COMPUTER CRIME 244 (1983); Donald G. Ingraham, *On Charging Computer Crime*, 2 COMPUTER/L.J. 429, 429–30 (1980).

107. Kerr, *supra* note 32, at 1602.

108. For example, a well-publicized event involving "pirate bulletin boards" between the time the act was first passed and the 1986 amendments sparked congressional concern over this type of computer crime, leading to the development of a provision in the Act regarding trafficking of stolen passwords. H.R. REP. No. 99-612, at 6 (1986); *see also* 1986 CFAA, *supra* note 89. Significant additions to the statute also came in 1994 to address the growing use of "worms" and "viruses" by computer criminals. Violent Crime Control and Law Enforcement Act of 1994 Pub. L. No. 103-322; 108 Stat. 1796, § 290001; 139 CONG. REC. S16,421 (1993).

109. In other words, it constitutes the purpose value of the legislative history that, once identified, can serve as the starting point for resolving statutory ambiguities. Eskridge, *supra* note 72, at 394.

programming.[110] Because code serves as the primary constraint on behavior, "the set of protocols, the set of rules, implemented or codified, in the software of cyberspace itself, which ... sets the terms upon which [one] enters[s], or exist[s] in cyberspace,"[111] circumventing code protections must be categorized as the misuse of a computer. As such, a code-based interpretation of authorized access aligns well with the contextual legislative history of the CFAA as prosecuting computer-misuse crimes.

In contrast, it is less clear that the agency-based approach targets computer-misuse crimes. In most cases using this approach, it is difficult to say that the person actually misused his computer in any way; instead, he was just using his computer normally, but for purposes of which his employer disapproved. In this sense, rather than capturing computer misuse, the agency approach more likely captures behavior that is traditionally normatively bad if not criminal—such as stealing trade secrets or breaching confidentiality—that just happened to be committed using a computer. Thus, the agency-based approach is not particularly consistent with the legislative history vision of the CFAA as a statute seeking to punish computer misuse.

Finally, while the contract-based approach to authorization may also often be inconsistent with the general legislative aim, it does have the potential to capture computer misuse in some circumstances. Contracts, of course, can range from the vague to the specific. Similar to the agency-based approach, a court that finds CFAA liability using a contract-based approach to authorization under a particularly vague contract or employee handbook—perhaps one that merely states that the employee should not act against the company's interests—is arguably finding liability for a traditionally normatively bad, if not criminal, offense. However, unlike with the agency-based approach, a more specific contract could be drafted that captures the legislative concern of the CFAA. That is, employers could specifically provide that using one's valid computer access to gather, copy, or transfer company information against the company's interest is a form of computer misuse that constitutes unauthorized access. A contract-based approach finding liability in such an instance is arguably consistent with the understanding within the legislative history of the CFAA as targeting computer misuse.[112]

For those that find general legislative goals as highly valuable in statutory interpretation, the insights above may be determinative, and the debate over the best approach will end here: with the code-based approach as the clear winner because it alone determines authorization based on whether the

110. Kerr, *supra* note 32, at 1644–45.

111. Larry Lessig, *The Laws of Cyberspace*, *in* READINGS IN CYBERETHICS 134, 136 (Richard A. Spinello & Herman T. Tavani, eds., 2d. ed. 2004).

112. Admittedly, the purist would argue that this is just redefining computer misuse to capture actions within the broader category of traditional crimes using a computer, and to some extent this may be true. However, if, as I argue below, there is some justification for deviation from a strict code-based approach to authorization, this form of contract-based interpretation, where liability is found only where there is a clear violation of a specific contractual definition of misused access, may be the best option for respecting the congressional expression that the CFAA targets crimes of computer misuse.

individual engaged in the misuse of a computer. However, there is yet another insight to be gained by taking a broader look at the CFAA's legislative history.

2. *A Legislative Grant of Discretion for Determining Authorized Access?*

In addition to clarifying the general legislative aim, a broader view of the CFAA's legislative history suggests a congressional intent to give courts greater discretion in determining the meaning of "authorized access" in employment cases.[113] Specifically, congressional inaction (in terms of both the failure to define key words and phrases and the lack of specific treatment of employment situations) as well as congressional confusion and ambiguity (as displayed in the changing nature of Congress's comments on the application of the CFAA to insiders) may indicate that Congress has left room for the courts to fill in the content of phrases such as unauthorized access in CFAA employment cases.[114]

First, Congress has neglected to clarify how authorization under the CFAA operates in employment-related computer crime, despite numerous opportunities. Although the CFAA has always had a definition section, Congress has never defined many of the key terms of the statute.[115] This failure to elaborate on key terms dates back to the original 1984 Act, where the only term Congress defined was "computer"[116] in order to avoid attacks on vagueness grounds.[117] The legislative history of the CFAA clearly establishes that Congress never defined many difficult and confusing, yet key, terms in the CFAA, such as "access," "use," and "without authorization,"[118] even in light of repeated pleas for clear definitions.[119] And although Congress did define "exceeds authorized access" in the 1986 amendments, this definition is not particularly informative.[120]

---

113. *See* William N. Eskridge, Jr., *Spinning Legislative Supremacy*, 78 GEO. L.J. 319, 324 (1989) ("The legislature itself might have a meta-intent that judicial interpreters exercise policymaking discretion.").

114. Notably, courts have opted for "liberal judicial interpretation" consistent with a statute's policy goals where legislative history provides little assistance as to the meaning of a disputed phrase in other modern statutes, such as the Superfund Act. *E.g.*, United States v. Aceto Agric. Chems. Corp., 872 F.2d 1373, 1380 (8th Cir. 1989).

115. *See* 18 U.S.C. § 1030(e) (2006).

116. 1984 CFAA, *supra* note 76, at § 2102(a).

117. This was despite the fact that that "[t]he whole issue of defining the word 'computer' ha[d] plagued the consideration of computer crime legislation since its early days." H.R. REP. No. 98-894, at 23 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3709.

118. *See* 18 U.S.C. § 1030(e).

119. Tompkins & Mar, *supra* note 79, at 464; Mitch Betts, *U.S. attorneys push to clarify vague '84 DP crime law*, COMPUTERWORLD, July 1, 1985, at 22.

120. *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (noting how the distinction between "without authorization" and "exceeding authorized access" is "paper thin").

Additionally, even with the increased law enforcement focus on employment-related computer crime,[121] Congress has never specifically addressed this type of computer crime and its particularized issues. Congressional awareness that the evolving nature of computer crime requires diligence in amending the CFAA is prevalent throughout the CFAA's legislative history,[122] and Congress acted early and repeatedly to amend the statute to cover new, specific types of computer crime and criminals.[123] Yet notably, Congress has never specifically targeted employee computer crime.[124]

Although many have criticized the informational value of congressional silence or inaction,[125] the type of inaction within the CFAA's legislative history may legitimately suggest a congressional intent to grant judicial discretion in defining "authorization" in CFAA employment cases. Much of the debate over the value of congressional silence in statutory-interpretation questions focuses on its use to establish that Congress has acquiesced to a particular judicial interpretation, often by the Supreme Court, through its inaction.[126] In contrast, the congressional inaction here is not argued to be in response to a specific judicial interpretation, but rather is simply a factual

---

121. *See* PROSECUTING COMPUTER CRIMES, *supra* note 3.

122. *See* 141 CONG. REC. S9422 (1995) ("The need to reevaluate our computer statutes on a continual basis is inevitable . . . ."); 132 CONG. REC. S14,453 (1986) (recording statements of numerous senators concerning how the law is adapting and that the amendments are to "address effectively known evils of computer misuse"); S. REP. No. 101-544, at 5 (1990) (discussing changes to the law to address worms and viruses); H.R. REP. No. 99-612, at 4 (1986) (stating that Congress is "clarifying the existing laws to deal with the emergence of a new type of computer abuse" through the amendments).

123. Congressional perceptions of computer criminals and the particular threats they pose appear to drive the language and provisions of the CFAA. In the early years of the statute, the focus was on "hackers," who were seen by Congress as prankster-youths who were in fact trespassers with the potential to cause serious problems. *See* H.R. REP. No. 99-612, at 5; H.R. REP. No. 98-894, at 10 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3695–96. A federal computer-crime act was seen as needed to both provide for prosecution of these hackers as well as deter their criminal activities. H.R. REP. No. 99-612, at 5–6. Similarly, a well-publicized event involving "pirate bulletin boards" between when the first act was passed and the 1986 amendments sparked congressional concern over this type of computer crime, leading to the development of a provision in the Act regarding trafficking of stolen passwords. *Id.* at 6; *see also* 1986 CFAA, *supra* note 89. Significant additions to the statute also came in 1994 to address the growing use of "worms" and "viruses" by computer criminals. Violent Crime Control and Law Enforcement Act of 1994 Pub. L. No. 103–322; 139 CONG. REC. S16,421 (1993). In 2002, the statute was again amended to make sure that it captured computer crimes committed by terrorists. *See generally*, COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, U.S. DEP'T OF JUSTICE, FIELD GUIDANCE ON NEW AUTHORITIES THAT RELATE TO COMPUTER CRIME AND ELECTRONIC EVIDENCE ENACTED IN THE USA PATRIOT ACT OF 2001 (2001), http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm.

124. *See* 18 U.S.C. § 1030 (2006).

125. *See, e.g.*, James J. Brudney, *Congressional Commentary on Judicial Interpretations of Statutes: Idle Chatter or Telling Response?*, 93 MICH. L. REV. 1, 66–67 (1994) (discussing the concerns raised by courts and commentators over the use of legislative inaction in statutory interpretation).

126. *See, e.g.*, William N. Eskridge, Jr., *Interpreting Legislative Inaction*, 87 MICH. L. REV. 67, 67 (1988).

silence in the face of requests for congressional clarification.[127] This type of inaction suggests that Congress may simply not want to figure out how authorization is to operate in these insider cases, opting instead to let the courts sort it out.[128] Thus, Congress's failure to explain the intended scope of the CFAA in employment situations, through either clarifying the key phrases of the statute or providing a specifically applicable amendment, provides some support for the conclusion that Congress may have implicitly determined that courts are more adept at assessing whether a particular insider was unauthorized and thus liable under the CFAA.

Congressional ambiguity and even confusion about insider authorization in the CFAA also suggests a congressional determination to leave the authorization question to courts.[129] Initially, Congress did attempt to provide some explanation of how authorization should operate in insider cases through discussions of legitimate purposes.[130] However, later references to insiders as unauthorized users are notably vague; in stating little other than that the statute covers "either outside hackers or malicious insiders" and that insiders must possess a higher scienter,[131] the references fail to provide a meaningful understanding of how authorization functions within the CFAA where the accessing party is an insider, such as an employee. This obfuscation suggests either that Congress did not understand or could not clearly articulate how authorization should operate where the person accessing was an insider. Regardless, the end result of the ambiguity appears to be that Congress left courts with greater leeway and responsibility in providing the content of the unauthorized access in insider situations such as CFAA employment cases.

Thus in addition to the general legislative aim of the CFAA, a second contextual insight can be gained from the CFAA's legislative history. We see that Congress has exhibited a high level of evasiveness and ambiguity when it comes to dealing with authorization in insider situations. That this has persisted in spite of admonishment by commentators and the development of competing approaches in courts may indicate a desire by Congress to leave the question of what determines authorization in employment situa-

---

127. *Cf.* Galbraith, *supra* note 9, at 368 (calling for congressional amendment to the CFAA to clarify authorization in cases involving public websites, which arguably are also "insider" cases).

128. *See* RICHARD A. POSNER, THE FEDERAL COURTS: CRISIS AND REFORM 290 (1985) ("Often when there are political pressures to do something about a problem but the legislature cannot agree exactly what to do about it, it will pass a statute to the effect (as well as the undisclosed purpose) of which is to dump the problem in the lap of the courts . . . ."); *see also* Eskridge, *supra* note 72, at 386.

129. Paul Diller, *Intrastate Preemption*, 87 B.U. L. REV. 1113, 1147 (2007) ("Legislative ambiguity is also frequently an intentional recognition of the limitations of the legislative process by the legislature itself. Legislation is necessarily forward-looking and cannot anticipate the circumstances that may arise years ahead concerning a particular application of legislation."); *see also* WILLIAM N. ESKRIDGE, JR., DYNAMIC STATUTORY INTERPRETATION 123–28 (1994).

130. *See supra* notes 76–84 and accompanying text.

131. S. REP. No. 104-357, at 9, 11 (1996).

tions open to judicial interpretation.[132] And, as discussed below, this possibility for courts to use greater discretion in the approach they take to authorization in CFAA employment cases suggests the need for a careful analysis of the policy implications of the alternative interpretations.

III. EVALUATING THE ALTERNATIVES

An important question now is how the two insights discussed above—the general legislative purpose of combating computer misuse and judicial discretion over the operation of insider authorization—should interact. This Part advances one reasonable alternative that incorporates both insights: a system in which the code-based approach serves as a default rule of interpretation for "authorization" within the CFAA, but is subject to courts' discretion to apply an alternative approach in CFAA employment cases when justified—in particular, when called for by a specifically applicable contract. Section III.A discusses the policy justifications for applying a code-based interpretation in most cases, while Section III.B evaluates the validity of both the agency-based and contract-based interpretations as alternatives in appropriate circumstances. Section III.C explores the practical operation of my approach.

A. *A Code-Based Approach as the Standard Default Interpretation*

The advantages of a code-based interpretation of authorization in CFAA cases are well documented.[133] Such an interpretation not only stays true to the general legislative aim of specifically combating computer misuse,[134] but may also have policy justifications supporting its use in CFAA cases more generally—that is, those that involve outsiders as well as insiders. Specifically, using a code-based approach in CFAA cases involving websites may provide a better balance between openness and privacy by not unintentionally capturing or chilling behavior that is arguably nonharmful.[135] Additionally, as the narrowest reading of unauthorized access, the code-based interpretation presents the least risk of raising due process concerns and issues involving the rule of lenity if it is carried over to criminal CFAA cases.[136]

---

132. *Cf.* Dov S. Greenbaum, Commentary, *The Database Debate: In Support of an Inequitable Solution*, 13 ALB. L.J. SCI. & TECH. 431, 499 (2003) (noting that congressional ambiguity regarding database legislation suggests a desire to leave much of the law open to judicial interpretation); Tiffany M. Wong, Comment, *Defendants' Standing to Oppose Lead Plaintiff Appointment Under the Private Securities Litigation Reform Act of 1995*, 2003 U. CHI. LEGAL F. 833, 846 (noting that silence in the Private Securities Litigation Reform Act with respect to the most adequate plaintiff presumption "raises the question of whether the text was intentionally left vague to give courts discretion").

133. *See* Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2258 (2004); Kerr, *supra* note 32, at 1651.

134. *See supra* Section II.B.1.

135. Kerr, *supra* note 32, at 1651.

136. Bellia, *supra* note 133, at 2258.

Considerations of judicial administrability may also militate in favor of a code-based approach.[137] Specifically, a code-based approach as the default interpretation of authorization within the CFAA may provide for greater predictability and require less judicial fact-finding, since the operation of authorization turns on something fairly easily ascertainable by potential parties and courts—whether there are code programs on the computer system, such as user name and password requirements, that the defendant needed to bypass in order to gain authorization. It is also notable that the code-based approach is the only interpretation of authorization that can be applied in all CFAA cases. That is, both the contract and agency approaches require the existence of a specific type of relationship that may not necessarily be present in a CFAA case involving a hacker or the user of a website. The universality of the code approach thus also supports its primacy as a default interpretation.

The previous considerations suggest that the code approach is the best default interpretation of authorization in CFAA cases generally, but the legislative history suggests that greater judicial discretion in the treatment of authorization in insider cases is permitted.[138] This raises the possibility that interpretations other than the code-based default could be appropriate in CFAA employment cases.[139] In this light, it is perhaps not surprising that courts employ a variety of interpretations to authorization in such cases. The question becomes, however, whether these other approaches are wise and justified as alternatives to the code-based approach in CFAA employment cases. This requires an evaluation of the merits of each alternative approach in such cases as well as an evaluation of how the use of such an alternative would function in relation to the code-based default interpretation of authorization.

B. *Evaluating the Merits of the Alternatives*

As noted in Section II.B.2, the legislative history of the CFAA suggests that Congress sought to give some discretion to courts dealing with authori-

---

137. *See* POSNER, *supra* note 128, at 289 (stating that considerations of judicial administration may be useful where there is uncertainty as to the correct statutory interpretation).

138. *See supra* Section II.B.2.

139. This notion that it is acceptable for the courts to branch out somewhat in their interpretation of the statute in these insider cases may even be supported under other jurisprudential theories of statutory interpretation. Although there are a wide variety of views on statutory interpretation, one clear divide exists between those that view judges as "honest agents," whose role it is to carry out the commands of the legislature by closely adhering to a statute's text and legislative history, and those that argue that courts should consider the cooperative nature of lawmaking, the importance of context, and the need for statutes to evolve over time. *See* ESKRIDGE, *supra* note 129, at 141–42; Eskridge, *supra* note 113, at 320–21 (1989). Arguably, many of the "honest agent" variety could find that courts should adopt a different interpretation of authorization when the case involves an insider; the legislative history suggests those situations are different and perhaps require a bit more independent judgment by the honest agent. *See* ESKRIDGE, *supra* note 129, at 124. Additionally, those who are more open to a dynamic, evolutionary perspective to statutory interpretation might argue that courts should have the opportunity to provide an interpretation that better responds to the different context present in the insider situation. *See id.* at 142.

zation in insider situations. Yet this discretion is not unbounded, and courts need to evaluate whether alternative approaches to authorization in the employment context extend the statute beyond what is beneficial from a policy perspective. This Section seeks to provide such an assessment of the two possible alternative schemes and ultimately concludes that in situations where deviation from the default code-based approach is permissible, the contract-based approach, when correctly used, best walks the fine line of providing flexibility to the CFAA while not overreaching its bounds.

1. *The Agency-Based Approach*

While the agency-based approach to interpreting authorization provides employers with another weapon against rogue employees who are pilfering confidential information,[140] its use nonetheless raises numerous concerns that may not outweigh its salutary characteristics. As previously noted, the agency-based approach does not neatly align with the general legislative aim of the CFAA.[141] However, there are concerns beyond this. Before adopting an agency-based approach, it is important to understand how common-law agency principles would operate in this particular statutory setting.[142] Such an analysis reveals that an agency-based interpretation has two fundamental flaws that counsel against its use as a discretionary alternative to a code-based interpretation: it employs particularly vague and malleable standards and may disturb established policy preferences in trade secret law.

The first problem with the agency-based approach centers on the considerable play in the joints that is inherent in common-law agency principles.[143] The law on fiduciary duties is not only situation specific,[144] but also notably elusive and nebulous.[145] The result is that courts have the opportunity to manipulate common-law agency principles to conform to the outcome they view as most fitting.[146] Moreover, since it is common for opinions that turn on

---

140. *See* Warner, *supra* note 27, at 12.

141. *See supra* Section II.B.1.

142. Agency principles should not be used to interpret words in a statute without a careful examination of the impact of such incorporation. *See* Deborah A. DeMott, *Statutory Ingredients in Common Law Change: Issues in the Development of Agency Doctrine*, *in* COMMERCIAL LAW AND COMMERCIAL PRACTICE 57, 83 (Sarah Worthington ed., 2003) ("[T]ransplanting common-law doctrines into statutory settings requires care and close attention to statutory purpose and the operative meaning of common-law doctrines.").

143. Other commentators have noted how "strikingly broad" the agency-based theory of authorization is. *E.g.*, Kerr, *supra* note 32, at 1633.

144. Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 DUKE L.J. 879, 879.

145. Robert Cooter & Bradley J. Freedman, *The Fiduciary Relationship: Its Economic Character and Legal Consequences*, 66 N.Y.U. L. REV. 1045, 1045–46 (1991); DeMott, *supra* note 144, at 879, 882.

146. *Cf.* Michael J. Phillips, *Employer Sexual Harassment Liability Under Agency Principles: A Second Look at* Meritor Savings Bank, FSB v. Vinson, 44 VAND. L. REV. 1229, 1255–56 (1991) (arguing against the use of agency principles in employment sexual harassment cases and stating that because of the poor fit between agency rules and sexual harassment law "courts tend to apply different rules in different settings, often in an apparently manipulative, result-oriented fashion");

agency principles to be cloaked in moralistic terms,[147] a result-oriented decision against a normatively—but not lawfully—wrongful defendant may go unnoticed. Arguably, these considerations about the nature of agency common law are more problematic where the principles are being used to determine liability under a statute—that is, in those situations we hope our judges to be serving merely as the "honest agents" of the legislative branch.[148]

The potential for manipulability, or even simply disparate outcomes, can be seen in the two leading cases favoring the use of an agency-based approach. *Shurgard* and *Citrin* rely on sections 112 and 387 of the Second Restatement of Agency to find that the authority that had been granted to the employee in each instance was terminated when the employee breached his duty of loyalty to the employer.[149] Once this authority was terminated via a breach of duty of loyalty, the access was "without authorization."[150] But the operation of authorization under these agency principles is open to manipulation. First, it is not clear whether termination of authority under these sections would render all computer access by the employee without authorization as soon as the employee breaches his duty of loyalty. One could imagine a situation where an employee who is downloading or deleting files contrary to the interest of his employer may otherwise still be performing his job.[151] A court could determine either that acquiring any adverse interest to his employer left him without authorization, or it could find that the employee's actions did not constitute a serious enough breach of loyalty to find a termination of authorization. Both outcomes are arguably allowable under section 112, which establishes that authority terminates "if, without knowledge of the principle, [the agent] acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[152] Arguably, a court could even invoke other agency rules—such as section 108(2) of the Second Restatement of Agency, which allows the revival of authorization "upon the restoration of the original situation"[153]—to manipulate the outcome. This inherent play in agency rules presents not only the opportunity

---

Dawn K. McGee, Note, *Potential Liability for Misrepresentations in Residential Real Estate Transactions: Let the Broker Beware*, 16 FORDHAM URB. L.J. 127, 150–51 (1988) ("[C]ourts are . . . impos[ing] broker liability for misrepresentation or nondisclosure on a result-oriented basis.").

147. *See, e.g.*, Meinhard v. Salmon, 164 N.E. 545, 546 (N.Y. 1928) ("A trustee is held to something stricter than the morals of the market place. Not honesty alone, but the punctilio of an honor the most sensitive, is then the standard of behavior."); *see also* Robert C. Clark, *Agency Costs versus Fiduciary Duties*, *in* PRINCIPALS AND AGENTS: THE STRUCTURE OF BUSINESS 55, 75–76 (John W. Pratt & Richard J. Zeckhauser eds., 1985); Robert W. Tuttle, *The Fiduciary's Fiduciary: Legal Ethics in Fiduciary Representation*, 1994 U. ILL. L. REV. 889, 896.

148. Frank H. Easterbrook, Foreword, *The Court and the Economic System*, 98 HARV. L. REV. 4, 60 (1984).

149. Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).

150. *Citrin*, 440 F.3d at 419–20.

151. Warner, *supra* note 27, at 20–21.

152. RESTATEMENT (SECOND) OF AGENCY § 112 (1958).

153. *See id.* § 108(2).

for inconsistent treatment of defendants under an agency-based approach to authorization, but also the potential for outcomes that are in direct conflict with legislative pronouncements: specifically, a court that finds authorization to be totally terminated in the above example would impose CFAA liability on an employee for carrying out normal employment duties or the nonharmful, non-employment activities that Congress specifically recognized should not be reached by the CFAA.[154] Thus even assuming that judges would not purposely exploit the malleability of agency rules, there is a justifiable concern that the agency-based approach is simply too open to judicial interpretation to serve as an adequate alternative interpretation of authorization in the CFAA.[155]

Another problem with an agency-based approach to authorization in the CFAA is that it potentially disturbs established policy preferences ingrained in trade secret laws. Trade secret laws require a showing that the information misappropriated or stolen derives independent economic value from being secret and is the subject of reasonable efforts to maintain its secrecy.[156] Not only is this a difficult showing to make in many employment cases, but other trade secret law hurdles make it even more difficult to get relief when an employee misuses confidential information.[157] These greater burdens reflect policy balancing: lawmakers want to protect proprietary information, but are also aware of the need for human capital to be mobile and thus do not want trade secret laws to unduly prohibit individuals from using "generic business knowledge to compete with former employers."[158] Although many CFAA employment-related claims are accompanied by claims of misappropriation of confidential information,[159] the CFAA claims are notably easier to bring, since "employers can bring CFAA claims without having to prove that the information wrongfully accessed was a

---

154. *See* H.R. REP. No. 98-894, at 15 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3701 (excluding unauthorized access for use that is "incidental," such as doing homework or playing computer games).

155. Notably, the Third Restatement of Agency tightens some of these conceptual gaps that present opportunities for differing outcomes because it evaluates whether authority was actually present in a situation rather than whether circumstances terminated it. *See* RESTATEMENT (THIRD) OF AGENCY § 3.06 reporter's notes (2006). Under a Third Restatement interpretation of access "without authorization," section 2.01 could be used to find that the employee never had authority for the specific action because it was unreasonable for him to believe that his employer wished him to take the action of, for example, deleting incriminating files or downloading confidential information that will later be used to compete with the employer. *See id.* § 2.01. Because the analysis would turn on whether the employee possessed authority for a specific access instance, it would not face the same issues as termination-based authority regarding the status of later instances of access. Arguably, however, the manipulability problem is not quite solved; a court could now simply use the Third Restatement construction rather than the Second, or vice versa, to reach the specific outcome they want.

156. 18 U.S.C. § 1839(3) (2006); UNIF. TRADE SECRETS ACT § 1(4) (1985).

157. *See* Chan & Rubiner, *supra* note 10, at 12.

158. H.R. REP. No. 104-788, at 7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4026.

159. *See, e.g.*, Black & Decker (U.S.), Inc. v. Smith, 568 F. Supp. 2d 929, 930 (W.D. Tenn. 2008), *interlocutory appeal granted*, No. 07-1201, 2008 WL 3850825 (W.D. Tenn. Aug. 13, 2008).

trade secret, [or] constituted confidential or proprietary information."[160] Moreover, under an agency-based approach, authorization hinges on a breach of duty of loyalty and that breach of duty of loyalty in turn hinges on the purpose for which one was acquiring the employer's information. As a result, it is not difficult to imagine that one could be liable under the CFAA for what essentially amounts to the misappropriation of confidential information yet has none of the difficulties that come with trade secret claims (i.e., proving independent economic value and reasonable efforts to maintain secrecy). Thus, a very practical concern with the agency-based approach to authorization in the CFAA is that it not only puts a new arrow in the employer quiver,[161] but an arrow capable of overriding traditional trade secret liability and thus disrupting established policy preferences in employment law.

In contrast to these two potential concerns, the potential benefits of the agency-based approach in CFAA employment cases may be slight. Notably, agency rules can function as a control mechanism, discouraging behavior that may or may not violate fiduciary obligations.[162] In this sense, of all three alternative approaches, the agency-based approach to authorization in CFAA employment cases conceivably would do the most to discourage the wrongful use of computer access by employees, since liability may attach any time the employee acts in a manner capable of being characterized as against his employer's interests. However, there may be reason to doubt the deterrent affect of the agency-based approach. For it to affect an employee's decisions, the employee would have to not only know about the existence of liability under the CFAA for unauthorized computer access, but also the operation of agency principles and even that the relationship with his employer is an agency relationship. Given that even judges often do not understand the nuances of agency law,[163] and because agency relationships may be formed even absent an agent's knowledge,[164] the general deterrent effect of using agency rules in the application of the CFAA is doubtful, making the potential benefit from doing so doubtful as well.

The problems noted above, as well as the fact that an agency-based approach does not align with the general legislative aim of the CFAA,[165] counsel against using it as the interpretation of authorization in CFAA employment cases. Whatever benefit can be gained from an agency-based approach is arguably not sufficient to overcome the concerns of malleable standards and negative policy implications.

---

160. Peter J. Pizzi, *Disloyal Employees: Computer Abuse Law Turns on Meaning of 'Without Authorization'*, N.Y. L.J., Sept. 5, 2006, at 5, 9.

161. Warner, *supra* note 27, at 13.

162. *See* J.A.C. Hetherington, *Defining the Scope of Controlling Shareholders' Fiduciary Responsibilities*, 22 WAKE FOREST L. REV. 9, 11 (1987).

163. *See* Phillips, *supra* note 146, at 1255.

164. GREGORY, *supra* note 14, at 5, (noting that agency relations may be created by "mistake"); *see id.* at 34 (discussing the creation of agency and the lack of formalities required).

165. *See supra* Section II.B.1.

2. *The Contract-Based Approach*

In contrast to the agency-based approach, a contract-based interpretation may be a justifiable approach to authorization in CFAA employment cases when deviation from the code-based approach is desirable. Though they focus primarily on the use of a contract-based approach in non-employment cases,[166] other commentators evaluating the use of a contract-based approach have expressed concerns worth exploring.[167] The main criticism of the contract-based approach is that it gives the computer-network owners too much power in regulating users of that network.[168] Yet even as the contract-based approach allows the owner to define authorization as he wishes, it nonetheless results in weaker regulation, since it is easier to bypass a contract-based protection than a code-based protection.[169]

All of these concerns, however, are related to the nature of the relationship between the computer-network owner and the user. Take, for instance, a situation where the computer-network owner and computer-network user are complete strangers with no prior interactions, brought together only out of the user's desire or need to access the owner's network or internet site. In such a situation, the concerns regarding the owner's ability to strong-arm access terms and the user's ability to easily circumvent those terms would be weightier. First, absent any relationship, the costs of negotiation over access terms would be high. As such, if access to the network or internet site is particularly valuable to a user, the network owner is inherently in a superior position with regard to defining the relationship and the nature of the parties' interactions. He could choose to condition access to his network on virtually any grounds the user is willing to agree to in order get the access he or she wants.[170] Additionally, not having significant past experience with this computer-network owner, the user may discredit the significance of her agreement to the access terms and misrepresent herself in order to bypass the contract-based access protection.[171] Indeed, this was the type of relationship on which the commentators focused when they expressed their

166. *See, e.g.*, Kerr, *supra* note 32, at 1650 (discussing the contract-based approach with respect to website owners and internet users).

167. Kerr, *supra* note 32, at 1646 ("Regulation by contract offers a significantly weaker form of regulation than regulation by code."); *see also* Bellia, *supra* note 133, at 2258 (discussing due process concerns raised by allowing a network owner's posted usage policy to potentially determine criminal liability); Galbraith, *supra* note 9, at 345–49 (criticizing the use of an employment contract to define unauthorized access in a CFAA case).

168. Kerr, *supra* note 32, at 1650. Because interpretations in the civil context can be applied to criminal prosecutions under the CFAA, this main concern feeds into other concerns—specifically, that the computer owner will be able to define the scope of criminality. *Id.* at 1651. And, if it is not clear to a user that he is operating under a contract, there is the potential for due process violations. Bellia, *supra* note 133, at 2258.

169. Kerr, *supra* note 32, at 1646.

170. *E.g.*, *id.* 1650 (discussing the click-through restrictions a computer network owner could create to define access).

171. *E.g.*, *id.* at 1646 (discussing how a seventeen-year-old can easily misrepresent her age in order to access a site that requires users to indicate that they are at least eighteen years old before access is granted).

concerns that the contract-based approach gives too much power to owners while providing only weak regulation.[172]

But, significantly, these are not the type of relationships and contractual circumstances that arise with employment cases. Instead, the relationships in employment cases are typically more established and structured. This difference provides the opportunity for parties to construct access contracts that are narrower and more likely to be adhered to, and thus perhaps less susceptible to the concerns that have turned other commentators off of a contract-based approach. For example, in one recent CFAA employment case, the employer and employee had an Employment Access Agreement that explicitly granted the employee authority and access to his employer's computers; it stated that the employee's authority and access would not terminate until the company took "corrective action for noncompliance, up to and including, as it may correspond, the suspension of [the employee's] individual Employee Access Agreement."[173] As a narrow agreement that clearly establishes the regulated action, this document suggests that the concerns of commentators about a contract-based approach to authorization more generally in the CFAA may not always be applicable in employment cases.

Additionally, a contract-based approach to interpreting authorization may have benefits in certain employment cases. As mentioned above, by enforcing the authorization definition in a contract explicitly geared toward defining certain wrongful types of access as misuse of access, courts would still be effectuating the general legislative purpose of the CFAA.[174] Moreover, an employment contract that clearly defines the employee's access rights—perhaps even in relation to the CFAA—could also serve to deter some employees from even attempting to use their computer access to copy proprietary information before leaving the company. These specific employment agreements could also make employers more aware of the importance of network security, potentially encouraging additional precautions that help reduce the societal costs of computer fraud.

These benefits, however, are likely best achieved through only the careful and conscious use of a contract-based interpretation of authorization in CFAA employment cases. Perhaps distracted by the debate among courts over the agency-based approach, not many courts have taken notice of the possibility of a contract-based approach.[175] As such, it is difficult to say

---

172. Bellia, *supra* note 133, at 2234–41; Galbraith, *supra* note 9, at 321–24; Kerr, *supra* note 32.

173. Defendant Timothy C. Smith's Reply in Support of his Motion to Dismiss at 3, Black & Decker (U.S.), Inc. v. Smith, 568 F. Supp. 2d 929, 933–34 (W.D. Tenn. 2008) (No. 1:07–cv–01201–JDT–sta), *interlocutory appeal granted*, No. 07–1201, 2008 WL 3850825 (W.D. Tenn. Aug. 13, 2008) (citing the Employment Access Agreement).

174. *See supra* Section II.B.1.

175. *See, e.g.*, *Black & Decker*, 568 F. Supp. 2d at 933–37 (outlining the divide between courts applying an agency-based approach and those applying a code-based approach and adopting the latter without substantial consideration of the employment agreements relating to the employee's authorization).

where courts should draw the line in finding or not finding an employment agreement as defining an employee's authorization to access a computer system. However, it seems clear that courts should tend toward only applying a contract-based approach where it is clear that the employment contract is narrow and not too one sided in terms of giving extensive power to the employer to determine authorization, as well as specific enough that an employee would clearly know when his actions were crossing the line into computer misuse.[176]

Although others have expressed concern about a contract-based approach in CFAA cases generally, these concerns may be muted in CFAA employment cases such that courts could reasonably find that the benefits of such an approach warrant its application. While the case law on this approach needs to develop more before we can have a full understanding of a contract-based interpretation of authorization, it may nonetheless stand as an appropriate alternative to a code-based approach in CFAA employment cases.

C. *The Code-Based Default with a Contract-Based Alternative in Practice*

Code-based interpretations of authorization in computer contexts are particularly appealing, because it is usually easy to determine whether a person had properly acquired a password (and thus was authorized to access) versus when they had improperly acquired access either by stealing a password or hacking into the system by bypassing security measures. However, courts have not consistently opted for a code-based approach to authorization in CFAA employment cases because factually the employee will almost always have code-based authorization, having been given a password or physical and technical access to a computer system as part of his job. The legislative history suggests that Congress was somewhat aware of how the insider situation complicates the authorization question and, as a result, gave courts more flexibility in determining what authorization meant in these situations. Yet greater discretion does not equal a broad, unfettered license, so courts should carefully consider the implications of applying alternative interpretations in CFAA employment cases. An analysis of the relative merits of alternatives to the code-based approach establishes that a contract-based approach in CFAA employment cases may respond to the issues Congress noted in insider authorization questions in the most reasonable and least problematic manner.

This conclusion, however, should not end the inquiry. Because contracts in CFAA employment cases can run the gamut from non-existent to specifically defining the situation at hand,[177] there still remains the question of

176. Indeed, an unconscionability analysis drawn from contract law could unnecessarily confuse the CFAA analysis and may be a factor that courts could take into account when deciding whether to use a contract to define authorization in a particular CFAA employment case.

177. *See supra* Section I.C.

when courts should deviate from a code-based default and allow a contract to determine authorization under the CFAA.

The easiest cases with respect to whether deviation from the default is appropriate arise on either end of the contractual spectrum of specificity. On one end of the spectrum, where there is no contract between the parties, the default code-based approach would be the only applicable interpretation. On the other end would be a clearly applicable contract, such as one that states: "Employee's authorization to access the computer system and information on the system terminates when employee misuses that access to copy, download, or transfer company documents to further activities against the interests of the company. Access in such instances will be unauthorized and subject to civil liability under the CFAA." Clear definition of authorized access as well as reference to the CFAA in a contract informs both parties and courts of the expectations and the operation of authorization such that deviation from the code-based default has little potential to be problematic.

Where things become slightly more difficult is in the middle of the spectrum, where there may be a contract, but the terms are much more vague and perhaps only marginally applicable to an employee's authorization to access the computer system. For example, we can imagine an employment contract that states, "Employees must keep all information confidential," or "Employees may only use company information and documents for business-related work." Arguably, even without reference to computer privileges, a court could determine that such contract terms establish that the employee's authorization to access information on a computer turns on whether they are keeping it confidential or business related.

Courts should be cautious when evaluating these contracts though, and before deciding to deviate from the code-based default, they should fully consider the implications of allowing these more vague terms to govern authorization. One consideration may be whether the use of a particular contract to determine authorization implicates agency principles. As an illustration, the confidentiality example above may come very close to using agency principles in that liability could turn on the employee's intent to breach his duty of loyalty in exposing confidential information. Because of the problems with importing agency principles into the statutory operation of authorization,[178] courts may be well advised to stick with the code-based default where the use of vague contract terms may result in agency law creeping into the authorization determination. Other considerations in the choice to use a contract to determine authorization may include whether (and how much) the parties were on notice regarding this provision and its potential use, whether there are positive deterrence effects in using the contract to define authorization, and whether the use of the specific contract to determine authorization fulfills the general legislative intent of the CFAA in terms of combating computer misuse.

In adjudicating these borderline cases, courts may also want to consider the potential systematic gains from only deviating from the code-based de-

178. *See supra* Section III.B.1.

fault and applying a contractual definition of authorization where the contract terms are specific and clearly applicable. In particular, the application of a code-based approach with deviation to allow contracts to determine authorization only where they are specifically and clearly applicable is analogous to the situation of penalty default rules. Penalty default rules give at least one party the incentive to contract around the default and should be used by courts where such a rule will result in the revelation of valuable information at a low transaction cost.[179] Notably, a code-based default places the burden of the rule on the employer. He either defines an employee's authorization in contractual terms that a court will employ in a CFAA case, or faces the risk that employees may commit some type of harm without the need to circumvent established code-based protections and hence not face liability under the default code-based approach. This default is likely to elicit valuable information; the employer who seeks to contract for a more robust meaning of authorization than found in the narrow, code-based default approach will, in the process, educate the lesser-informed employees as to the extent of their authority to access the computer systems.[180] Additionally, because employers are likely to know the kinds of access they do not want to extend to their employees and may already have employment contracts that can be easily adapted to cover computer system privileges, the transaction costs of getting this information are likely low. Thus where the code-based definition operates similarly to a penalty default rule, it gives computer-system owners the incentive to contract for a more situation-specific definition of authorization when they foresee the possibility that a code-based interpretation will not suffice to protect against computer misuse by certain users. Such a situation is most likely to arise in employment contexts and would likely result in more informed employees and clearer ex post court decisions on employee liability under the CFAA. By only deviating from the code-based default where a contract provides a very specific, clearly applicable definition of authorization, courts foster a situation similar to that seen in penalty default rules. Moreover, carefully structuring the operation of authorization in such a manner is likely to be beneficial in CFAA employment cases.

Ultimately, the decision to deviate from the code-based default and instead base authorization on a contract will be extremely fact specific and within the discretion of the court reviewing the case. Unfortunately, there is little case law using contracts in CFAA employment cases that could help courts determine whether deviation is appropriate. Instead, courts must rely

---

179. Ian Ayres & Robert Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules*, 99 YALE L.J. 87, 97, 128 (1989).

180. Information-eliciting penalty default rules that place the burden on employers have been found beneficial in other employment contexts where the default offers (1) more protection for employees who are generally ignorant of the laws governing their employment relationships and (2) forces the better informed employers to educate employees about the terms governing the employment relationship. Rachel Leiser Levy, Comment, *Judicial Interpretation of Employee Handbooks: The Creation of a Common Law Information-Eliciting Penalty Default Rule*, 72 U. CHI. L. REV. 695, 697–98 (2005).

on their own judgment, bolstered by the considerations noted above, to determine whether the contract in a CFAA employment case should be used to define authorization in a specific case.

CONCLUSION

While the current state of confusion over the operation of authorization in CFAA employment cases is understandable due to the general and vague language within the statute, it is not an ideal situation for employers, employees, or courts. Specifically, the different interpretations often lead to disparate outcomes in terms of employee liability. Moreover, the use of an agency-based interpretation may be particularly problematic. It not only fails to further the CFAA's general legislative aim of combating computer misuse but also has particularly vague and malleable standards, which may disrupt established policy preferences of trade secret law. Until Congress gives better directives, courts should use the approach outlined in this Note in CFAA employment cases—a default code-based interpretation from which courts can deviate when a contract provides for a clear determination of the employee's authorization to access a computer system.

Considerations beyond the text suggest that the best approach to CFAA authorization questions generally is the narrow, code-based approach, which determines authorization on the basis of whether code-based protections had to be bypassed in order to gain access. Yet the legislative history also suggests that courts can use some discretion in defining authorization in employment situations to better tailor the CFAA to the more complex insider situations. The contract-based approach may then appropriately substitute the code-based default interpretation in certain CFAA employment cases. Cautiously deviating from the code-based default and using the contract-based approach when the governing contract clearly and specifically applies may help employers and employees better adjust their behavior and expectations with respect to computer use in the employment setting.